Claim History

The Examiner rejected claims 1-10 and 12-30 under 35 U.S.C. § 103 over Smith in view of Boebert et al.

Status

Claims 17-27 cancelled by the present amendment and claims 32-37 have been added. Independents claims 1, 12, 28, 31 and 32 with corresponding claims depending therefrom will remain for further consideration.

35 USC § 103

Claim 1 as amended now recites that the escrow encryption is <u>only</u> applied to packages for addressees that do not have a public encryption key. If an addressee has a public encryption key, then the package only receives a public key encryption "upon a determination that the addressee does have a public key, encrypting the package with the addressee's public key and not encrypting the package with an escrow encryption key." The encryption key is also further defined to be not equal to the generated "new" public encryption key, "said new public key is not equal to said escrow encryption key." The cited reference to Boebert merely shows a storage system for encrypting a file, namely any file that is saved. There is no investigation to determine whether the addressee has a public key on file. Boebert merely shows saving every file under a public key architecture. This teaches away from the current concept, which is to send out a file under the public key encryption if one is on file, or using an escrow encryption to prevent unauthorized access to a file while a public key is being generated. The concept of the current invention is that

instead of making the sender wait until an addressee public key is available, the system provides a unique escrow key that can be used to encrypt the message until such time as a public key is available. However, the sender is relieved of the need to wait for such a public key. A system using the Boebert invention would necessarily encrypt every message and every stored file encrypted. In contrast, the current invention requires a check before storing a file to determine whether encryption is needed, "searching at least one database to determine whether the addressee has a public key in order to determine the type of encryption to be performed on the package." While the Applicant still maintains that the encryption of Boebert is not an "escrow encryption key" as defined by the application, for at least the reason that Boebert does not test for prior encryption prior to storing files, the claims should be allowable for at least this reason.

Additionally, it is not understood what Boebert would add to Smith or why such a combination would be desirable. Smith already using a secret key to encrypt a document as it is received. Boebert at best teaches encrypting every document that is stored regardless of whether the document is already encrypted or not. The Delivery server of Smith either receives all documents whether a public key encryption is performed by the sender and stores them on the Delivery Server while they are processed and then forwards them to the recipient, or the Delivery Server does not store any documents, but merely forwards them. In either case Boebert would teach Smith (if anything) to either encrypt all of the documents or none of them. If Smith does not store documents (for instance in RAM or on a "hard drive"), then Boebert teaches Smith nothing and there is no reason to combine the two, except in hindsight. There is no teaching in Smith that documents are "stored" any differently for documents (e.g., in RAM) where the public encryption is known versus those where it is unknown.

There must be also a teaching in the references which would motivate one to combine the references, not merely that a benefit would occur by combining them ("hindsight"). *There must be a suggestion or motivation in the prior art to modify a reference* to satisfy the claimed invention. In re Gordon, 221 USPQ 1125, 1127 (Fed. Cir. 1984). *"The mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification."* Id. (emphasis added) "When an obviousness determination is based *on* multiple references, there must be a showing of some 'teaching, suggestion, or reason' to combine the references...Although a reference need not expressly teach that the disclosure contained therein should be combined with another the showing of combinability, in whatever form, must be *'clear and particular.'* ", Winner International Royalty Corp. v. Wang, 202 F.3d 1340, 1348-1349 (Fed. Cir.), cert. denied, 530 U.S. 1238 (2000)(emphasis added) It is not clear why Smith would want to store the documents under a Boebert type encryption since the documents are already encrypted. There is also no teaching in Boebert why Smith would want to store the documents to make them more "secure" than the encryption provided by Smith. Smith merely assigns an addressee public key ("secret key") to the document and then sends it to the addressee.

Claim 12 likewise requires that the determination of whether to apply an escrow encryption is performed by checking a directory for an addressee's public key and then applying a public key encryption or an escrow key encryption as needed.

Claim 28 requires that the escrow encryption key be applied only in response to a determination that the addressee does not have a public encryption key. In Smith, every document, whether a public key exists or not, is forwarded to the delivery server, and thus

would be stored in the delivery server, and in view of Boebert would be stored with the same encryption whether or not a public key exists for the recipient. Smith sends a document to the server using a secret key 40 (Col. 4, lines 62-68) Under Smith and Boebert, this would be the same encryption key for every document as no query has yet been made as to whether a public encryption key exists.

Independent Claims 31 and 32 further specify that the escrow encryption is added only after a determination whether the addressee has a public key. Boebert at best teaches that every file should be encrypted as transfer occurs between two computers. There is no teaching of adding a selective encryption.
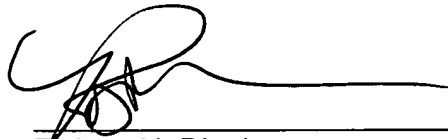
For at least these reasons, the claims should be allowable over the art of record. The dependent claims have additional recitations which must be considered, but should be allowable for at least the same reasons as the independent claims.

Summary

Applicants have made a diligent and bona fide effort to answer each and every ground for rejection or objection to the specification including the claims and to place the application in condition for final disposition. Reconsideration and further examination is respectfully requested, and for the foregoing reasons, Applicant respectfully submits that this application is in condition to be passed to issue and such action is earnestly solicited. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Robert N. Blackmon, Applicants' Attorney at 703-684-5633 to satisfactorily conclude the prosecution of this application.

Dated: December 22, 2004

Respectfully submitted,

Merek, Blackmon & Voorhees, LLC
673 S. Washington St.
Alexandria, Virginia 22314
Tel. 703-684-5633
Fax. 703-684-5637
E-mail: RNB@ BlackmonLaw.com

Robert N. Blackmon
Reg. No. 39494
Attorney/Agent for Applicant(s)